

Dear Mainer,

I am sure that I can't tell you anything new about the Internet. You've probably used computers since you were old enough to reach a keyboard. I am also sure that you know quite a bit about being smart and safe on the Internet. There are risks associated with Internet usage. Others use the Internet to victimize people your age. I hope you will take some time to read this booklet, which will confirm two important safety points: First, it is easy to deceive online; second, when you post online, nothing is private, ever. Anyone can share everything you give them with anyone anywhere in the world.

Online danger comes from many places. You may find yourself in an unsafe situation when strangers ask to add you as a friend, or when you have accidentally given out too much private information, such as your address or photographs. Sometimes, the danger comes from harassment between people you go to school with, play with or live near. Sometimes, it may be directed at you. Sometimes, you may be causing it without knowing you are.

Any of these situations can spin out of control. Please remember: Don't react. People who harass others feel powerful online. They just want to get a reaction - any reaction. Don't join in. Instead of contributing to rumors, ask yourself how you would feel if these were rumors about you. Sending hurtful or untrue information to others is just as bad as starting a rumor yourself. Stand up to unkind behaviors by peers. By showing the courage to speak up, you take some of the abuser's power away. Say something supportive to the target or tell an adult you trust. Do not engage in conversation with someone if you suspect they are dangerous. Save the evidence. Save upsetting information and bring it to someone you trust. And never, never post or send information or photos that you do not want your family, your friends or anybody else to see.

The most important thing is to stay smart. Ask questions. Is this relationship moving too fast? Would I disclose this information to another person if it wasn't on the Internet? Where can I search to prove the accuracy of this statement? Would I want my teacher or future employer to see this photograph on the Internet? How do I back out of this situation if necessary?

Remember, stay alert and stay in touch with people you trust. The

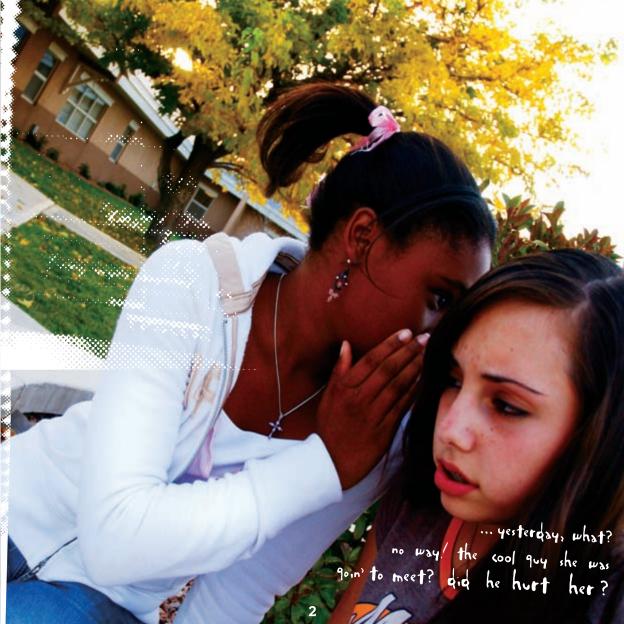
Internet is a powerful tool that brings the world to your desktop. We all just want to make sure you use it

safely and responsibly.

Thank you,

Thomas E. Delahanty, II United States Attorney District of Maine





WHAT'S THE PROBLEM?

The Internet can be a really great tool, fun to surf in your spare time, and totally entertaining. But remember, some things are just too good to be true.

Unfortunately, we live in a world where people sometimes take advantage of others, especially youth. It's good to be prepared; this may happen to a friend or a sibling. Anything on the Internet, whether it's chat rooms or web sites, that attracts you and your friends will also attract abusers, bullies and predators.

>>> Read on.

Many predators, people searching for young adults and teens to rape, kidnap or harm, now use the Internet as their tool of choice. Instead of doing research, like you are doing for that English paper, a predator uses the Internet to find victims. Predators communicate through chat rooms and instant messaging seeking to develop relationships with young people. They seek the trust of young people. When a trust forms, they ask to meet somewhere to check out a movie, window shop or

get something to eat. Typically, a predator does all this while posing as a young adult or teenager himself.

Who are the cyber predators?
Not who you think:

- >> Most are male
- >> Above average intelligence
- >> Above average incomes
- >> Have a successful career
- >> Most are white
- >> Have computer knowledge
- >> Many have children of their own
- >> Have no criminal history related to sex crimes
- >> Most are older than 26

HOW THEY LURE YOUNG PEOPLE:

Predators use the anonymity of the Internet to talk to young adults. They look for clues to figure out what you like, who you are and sometimes, even where you live. Too often, it's made easy because information has been volunteered by young people.

1/ USER NAMES / SCREEN NAMES:

While a user name or screen name seems like a pretty innocent thing, it can be a gold mine of information for the viewers. You might think about your favorite bands, pets, hobbies and sports as part of a user name or screen name. But by doing so, what information have you given someone who may want to hurt you to use?

User name: Abercromshoper89

This tells the viewer that you like to shop, Abercrombie and Fitch is a favorite of yours, and that you were born in 1989.

User name: <u>Drisonerofhermione</u>15

This tells the viewer that you are a Harry Potter fan, you especially like the character Hermione Granger, and you are likely 15.

Armed with this information, someone who may want to friend you in order to harm you will talk to Abercromshoper89 about shopping and fashion while talking to prisonerofhermione15 about Harry Potter and magic.

It may not seem important, but providing this information helps a potential abuser learn how to become a trusted friend and is unnecessary and potentially dangerous.



WHEN CHOOSING A USER NAME OR SCREEN NAME, think of the game "MadLibs."
Try using one of the following formulas to select a user name:

>>> Adjective + noun

stuffedninja

>>> Size + animal

minielephant

>>> Season + noun

NOT your age, phone number or address

>>> RANDOM number + ice cream flavor
45cookiedough

>>> Actor's name + action verb

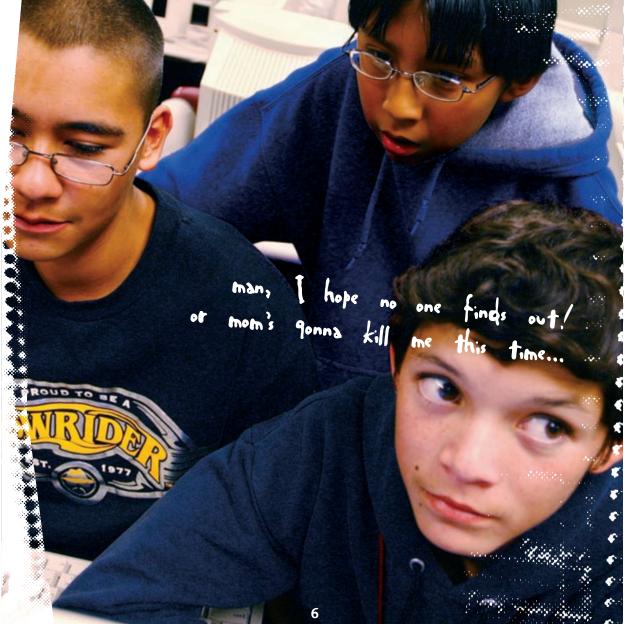
Travoltadancing

>>> Color + foreign food
pucebaklava

A user name or screen name with a random selection of words such as "Soupshoe" is much better than a potentially descriptive identifier such as "Missy1981". Make sure your user identifier doesn't relate to you, your age, your school, your location, or your interests.

and have fun with it!





2/ PROFILES:

Profiles can provide abusers and bullies with a lot of useful information. Profiles ask for information like your real name, birthday, address, phone number, hobbies and what school you go to. Filling out this information is meant to be useful to other teens and young adults who are looking for people to chat with who are interested in the same things. The problem is that those who want to manipulate you use personal information to gain your trust. Filling out profiles is not required to use most chat programs. To protect yourself, fill out profiles only on sites that allow you to control who has access to the profile.

3/ WHAT YOU SAY:

Some abusers will do something called "cyberstalking" (and yes, it's as scary as it sounds). An abuser will go to a teen or young adult chat room and pick a user name to follow through chat rooms. The abuser will slowly accumulate information about that user by simply reading what they are chatting about with other chatters. Young adults and

teens face many problems with peer pressure, parents, friends and other family members. Chat rooms seem like the perfect place to gripe about all those people who are disturbing your life, but watch out for people too anxious to relate. Often, abusers will play on your emotions by saying they went through the same thing.

4/ SELLING STUFF:

By selling things online, you can always make a quick buck off of things that you no longer use. But selling things can also provide dangerous information. Sometimes, a seller will provide their telephone number so that people interested in purchasing can call and ask questions about the item. Predators will use your telephone number to track you down. Providing your phone number not only identifies the state you live in, it also can lead to your doorstep.

THEIR TECHNIOUES:

Identifying a cyber predator is difficult because they sound like anyone else. Chatting online can be really fun and can be a quick way to make new friends, but it might not be the safest way. Predators, bullies and harassers have many techniques that they use to convince you that they are just like you, can relate to your problems, and would like to become your real friend instead of your online buddy.

Giving you special stuff:

Sometimes there are things that you may or may not want to see, like Playboy pinups or other sexually explicit material. Sometimes curiosity gets the best of us, but safety is always the most important thing to remember. When an online buddy sends you sexually explicit material,

whether you want it or not, it is smart to stop speaking to that buddy. Predators use this technique to scare or befriend you. Almost all of the time this material is unwanted. but if you continue to speak to this person, they will push you to do more things than just look at inappropriate material. Ending the conversation will tell that person that you are not interested in what they have to offer as an online buddy any longer.

Pretending:

As stated in the previous sections, abusers will often disguise themselves as teenagers and young adults. Sometimes they will let you know that they are adults, but most often they will befriend you online as a peer. These people can be very convincing and, without realizing what you have done, you may befriend someone who wants to

hurt you. There really is no way to know who is your same age and who is an adult, but being safe means ending communication with any online buddy if they begin to harass you. Remember, never give out too much personal information (not even an email address) and if anything mean or inappropriate happens, don't be afraid to tell your parents.

Threats:

If an online buddy begins to threaten you because you refuse to meet him or speak to him anymore, the best thing to do is tell your parents or a trusted adult. Bullies exploit any weaknesses they can find. Their objective is to make you do what they want, whether or not you want it. Getting advice from an informed adult will help you make the right decision and will make sure you stay safe.





User name tracking: Searching chat rooms or reading your blogs (online journals) are easy ways for anyone to learn how to talk to you and earn your trust. By following you through chat rooms, an abuser can gather information about you and make you feel comfortable enough to talk to them about anything, even revealing secrets. Beware of someone who knows everything about conversations you have been having or is quick to sav "the same thing happened to me."

Photographs:

Putting photographs online is becoming more and more popular, especially with chat rooms, blogs, and online social networks like "myspace.com." Unfortunately, there are a number of reasons why photographs are a problem:

- Combining a photograph with personal information can make it extremely easy for a dangerous person to find his way to your school or doorstep.
- Photographs can be manipulated—your face put onto another person's body in a sexually explicit photograph—and posted for anyone, including your parents, to see.
 - It is important to understand that a predator wants a picture of his prey. He will ask for a photo. He may ask for you to pose partially or completely undressed. If you send a picture of yourself that you would not want your parents or friends to see, it can be used to blackmail you into sending more. A predator is trying to control the person he is preying on. This is not a relationship about love; it is about control.

Pictures may be fun, but make sure that you post pictures only in places where people you know can view them. Be very careful when putting your photo online.

Email:

Sometimes you meet people who you really like online and you want to talk to them more than just in chat rooms. Giving out your email address or instant messaging screen name can be a good way to keep your conversation private. But be careful when you give out your email address. Your email address is personal, and it is unsafe to give it to online buddies because they can use it to discover more information about you. Limit the people who have your email address to friends and family; try not to give it to people you meet in chat rooms, and set your chat profile to not display your email address.



Predators groom their victims.
The objective of grooming is
to manipulate the victim into
behaving in whatever manner
the predator wants.

- 1 Charlie starts chat, expresses feelings that the predator can easily pick up on.
- 2 Predator begins "grooming" by expressing empathy to gain the kid's trust.
- 3 Charlie further expresses trust in the person he/she is chatting with, encouraging the predator.
 - 4 Further expression of empathy from predator.
 - 5 Charlie's frustration is evident to the predator who takes full advantage of Charlie by portraying himself as a trusted confidant.
 - 6 Predator offers a way to entice Charlie.

- Charlie89: my mom sux!

 its her falt that my

 parents are gettin divorced
- 2 PREDATOR: i no. my parents r2.
 - C: we never have \$\$ nemor
- 3 C: evry time i need somethin she says the same thing "we cant aford it"
 C: when my parents were 2gether i could buy stuff
- 4 P: me to. i hate dat.

C: now i cant

- C: i w8ed 6 mos for this game to come outC: my mom promisd mewed get it.
 - C: can i get it now? nope.
 - C: we dont have enuf \$\$\$.
- my mom sux!
- 5 P: wow, thats tuf
 - P: i hav a realy cool uncle
 - P: buys me things all
 - the time
 - P: he has lots o \$\$\$

C: ur sooooo lucky!

6 P: i got an idea. ill see if hell by it 4 u.

C: really? thx man!

P: brb gonna call him

8 P: w00t! he said k

C: wow realy? thx i
cant bleve it.

9 P: where do u live?

C: ptlnd, me u?

10 P: portsmouth, nh uncle 2.

ne malls near u?

C: maine mall.

P: ive herd of that one.
Saturday ok?

C: sounds good.

12 P: b ther at 12

C: k. meet at the game store.

P: k!

C: well g2g.

thx again dude

C: this is awesome!

C: TTYL!

P: 18r



- Of course, there is no "rich uncle."
 The predator gives that impression to Charlie by waiting for a period of time before sending his next message.
- Predator expresses excitement, tells Charlie the "uncle" will buy the game.
- 9 Predator starts asking for clues about Charlie, begins the process of scheming to find out where Charlie is to arrange a face-to-face meeting.
- The predator will place himself in close proximity to Charlie, regardless of his actual location.
- Charlie has actually just determined the final meeting place without realizing the danger he/she is in, even though trust has been built up with the new "friend."
- Predator finalizes the meeting.



The predator now has all the information he needs to meet you face-to-face.

Here's an example of an online chat you could experience and how you might find yourself being "groomed" by a cyber predator:



388888

SOCCF9F129 is chatting with a potential predator. WHO



Bob174: Hi

Soccrgr129: Hi

Bob174: ASL?

Soccrgr129: 13/f/usa.u?

Bob174: 14/m/usa

Soccrgr129: mm.. guess not

Bob174: y r u not at school?

Soccrgr129: day off. yay:)

Bob174: kewl. so ur home alone?

Soccrgr129: ya.parents r at work

Bob174: do u have a bf?

Soccrgr129: no

Bob174: do u want 1?

Soccrgr129: yes...:)

LikeMikey22: Hi

Soccrgrl29: Hi

LikeMikey22: asl?

Soccrgrl29: 13/f/usa.u?

LikeMikey22: 14/m/usa. u like soccer?

Soccrgrl29: yea, it's my fave sport. i'm a forward

LikeMikey22: cool. me to :)what else do u like to do

Soccrgr129: hang out with my friends, go shopping at

the mall, go to the movies. u?

LikeMikey22: skateboard, hang out, play

hackeysack, watch tv

Soccrgr129: cool. skateboarding looks

like fun but i bet i would fall

LikeMikey22: it's not that hard

Soccrgrl29: maybe i'll try it someday:)

maybe i'll try it someday...

The answer: Both Bobl74 and LikeMikey22 could be potential predators. But the most recognizable predator is Bobl74. He asks highly personal questions and wants to know if Soccrgrl29 is alone.

1 in 7 young people has received unwanted sexual solicitations online

1 in 3 young people
has been exposed to
sexually explicit

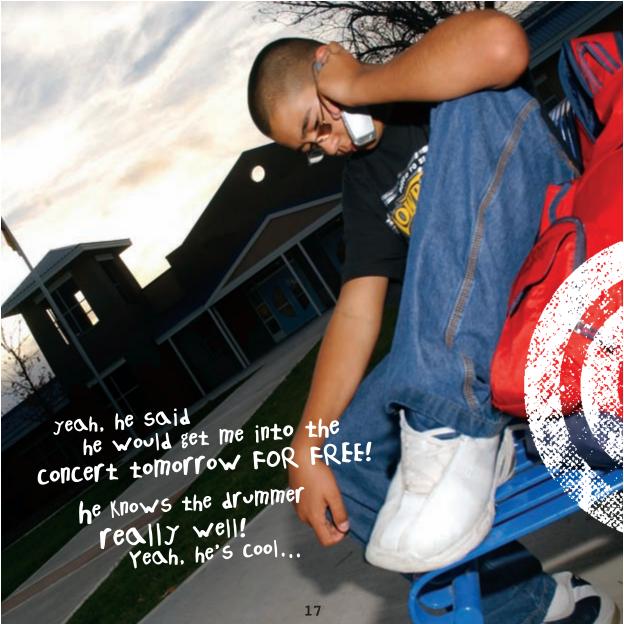
pictures online without seeking or expecting them

1 in 17 young people has been <u>threatened</u> or harassed online

> 1 in 25 young people has received an aggressive solicitation



to meet somewhere





& their POTENTIAL CONSEQUENCES:

Whether online or offline, almost everything you do has a consequence. If you do it online, it, and the consequences, may be memorialized forever. Always ask yourself what the possible long term consequences could be—no matter how far-fetched. Remember, anything you post on the Internet may one day be seen by the admissions officer from your favorite college, a future employer or even a future boyfriend or girlfriend.

1. Posting pictures of yourself on the Internet

In addition to allowing anyone to get a look at you, digital photo manipulation can put your face on another body, in any graphic or degrading situation. When such a photo is in the possession of an abuser, it can have devastating consequences. The abuser might threaten to send the picture to your parents or spread it all over the Internet unless you do as he says.

2. Posting on blogs and social networking sites

These features are virtual diaries that give viewers a more intimate look into your thoughts, feelings and vulnerabilities. This information could be exploited by cruel or dangerous individuals. Be aware of facts you post that identify your school, community or family.

3. Responding to postings that are belligerent or harassing These messages are often posted by the author simply to get a reaction - any reaction. If you do respond, you may open yourself to harassment. Don't join in. Instead of contributing to rumors, ask yourself how you would feel if you were the target. Forwarding hurtful or untrue information is just as bad as starting a rumor yourself. Stand up to unkind behavior by peers. By showing the courage to speak up, you take some of the abuser's power away. Say something supportive to the target or tell an adult you trust. Do not engage in conversation with someone if you

Save the evidence. Save upsetting information and bring it to someone you trust.

suspect they are dangerous.

4. Chatting with strangers in a chat room

Giving out information to people online is just as dangerous as giving the same information to a stranger you meet on the street, maybe even more dangerous.

5. Using a webcam

By allowing people to view your webcam, you are essentially opening the shades to your home or your bedroom and allowing anyone to watch you through that window. Predators and harassers will use what they see to take advantage of or harass you. Once images of you are online, they are online forever.

6. Accepting webcam views

By accepting an invitation to view live webcams, you could be exposed to unwanted nudity and sexually explicit video which could be disturbing. Remember, that 16-year-old that is inviting you to see him is more likely to be around 50, overweight and hairy.

7. Arranging a face-to-face meeting with someone you've

met online

Since it is not possible to know who you are really talking to online, you may be unpleasantly surprised when you discover that person's true identity. It is very possible that the person has misled you with the intent to harass or hurt you, even to molest, rape, kidnap, or kill you.

8. Downloading pictures from an unknown source

Downloading a picture may bring hidden viruses, which may destroy your computer, or place "cookies" that allow the sender to track where you go on the Internet, as well as key stroke trackers that may be used to steal your identity.

9. Filling out online profiles

Filling out profiles will allow others to see personal information about you, such as your real name, phone number, address, school name, etc., and will allow the abusers to "find" you offline.



CYBER SAFETY GUIDELINES:

Help catch abusers, bullies and harassers and protect your friends. Even if you are safe, someone you know may be the next target. Report any of the following to a local police officer.

3

3

- >>> Threats, bullying, harassment
 save the communication by
 copying and pasting into a
 text file.
- >>> Sexually explicit pictures
 or streaming video do not print it or send it.
 Save the information.
- >>> Sexual solicitation save the communication by
 copying and pasting into
 a text file.

Don't stay in an uncomfortable or dangerous situation online. You might hesitate to tell your parents because they may not approve of how you got into the situation. But you should realize that a bad situation could get worse if you ignore it.

Know your social networking privacy settings.

>>> You can limit access to your information, photographs and conversations. Only those you trust should be close to you online.

>>> When starting new friendships, always ask yourself: Is this friendship moving to intimate subjects too quickly? Is this too good to be true? Would I answer that question if someone asked me face to face? Do I want my future employer, boss or coach to see that picture?

Share these guidelines with your friends and siblings.

You can get more information about online safety at:

www.mcctf.org/InternetSafety.htm 22 www.maine.gov/ag/



www.mecasa.org

STATEWIDE SEXUAL ASSAULT CRISIS AND SUPPORT LINE 1.800.871.7741 TTY 1.888.458.5599

This is a confidential 24-hour toll-free hotline accessible from anywhere in Maine.
Calls are automatically routed to the closest sexual assault support center.

what? really?

he said he's gonna copy the latest CD for you?

oh sweet, man. you are meeting him at the park?

Yo. Later.

which of these two people should dirt-rider-15

be suspicious of



dirt_rider_15: hey
mx racer45: ASL

dirt_rider_15: 15/m/me

.dirt_rider_15: u

mx_racer45: 17/m/nh

mx_racer45: darn hoping u would be girl

mx_racer45: but no problem, u ride moto thou?

dirt_rider_15: yeah 4 fun

mx_racer45: awesome me 2 mx_racer45: what u ride?

dirt_rider_15: kx250

dirt_rider_15: u?

mx_racer45: yz400

mx_racer45: u have pic of it?

dirt_rider_15: yeah, I send it.

dirt_rider_15: u have 1?

mx_racer45: great look n bike

dirt_rider_15: yours 2

mx_racer45: I liv in manchester, nh, where u liv?

dirt_rider_15: lewiston, me mx racer45: where that?

dirt_rider_15: between portland and augusta

mx_racer45: cool

mx_racer45: maybe we can rid some time

dirt_rider_15: cool

The answer: Both mx_racer45 and moto-boy77 could be potential predators, pitcures moto-boy77 could be potential predators, but



moto-boy77: Hey dirt rider dirt_rider_15: Hey moto-boy77: ASL dirt_rider_15: 15/m dirt_rider 15: u moto-boy77: 17/m, moto-boy77: 2 old for u? dirt_rider_15: no moto-boy77: I c u ride motocross dirt_rider_15: just 4 fun moto-boy77: cool moto-boy77: I also ride 4 fun, moto-boy77: I used to compete dirt_rider_15: y u stop? moto-boy77: 2 busy moto-boy77: where do you live, maybe we can go dirt_rider_15: I am not supposed to say moto-boy77: Ok but I thought it might be fun if showed you some cool tricks dirt_rider_15: I guess it would be ok dirt_rider_15: lewiston, me moto-boy77: Is that near portland? dirt_rider_15: kinda howd u know? moto-boy77: I have friend in portland that I am going to visit in a few weeks moto-boy77: do you want to go ridding then? dirt_rider_15: that would be cool moto-boy77: u have pic? moto-boy//: u nave Pic.
dirt_rider_15: yeah why? moto-boy77: I like 2 no who I/m talking 2 dirt_rider_15: o, I'll send it dirt_rider_15; u have 1?

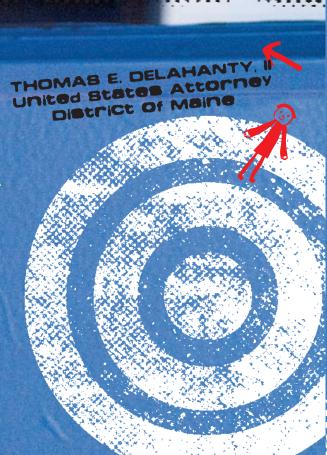
OTHER IMPORTANT INFORMATION to protect you and your family Chine

You are responsible for what you post on the Internet. To avoid unsafe situations for you, your family or for others, THINK BEFORE YOU ACT. Understand what it means to be a critical consumer of the Internet.

IF SOMETHING SEEMS TOO GOOD
TO BE TRUE, it probably is. Don't
believe someone wants to give you
money for nothing.

FORWARDING A MESSAGE MAY PERPETUATE A MYTH. Don't help spread another "Urban Legend" around the Internet. Learn the truth at websites like www.snopes.com or do an Internet search. Spreading rumors is wrong offline and it can be even more harmful online because it can spread faster.

SUCCESSFUL FRAUDS AND SCAMS
LOOK LEGITIMATE. Don't let an
authentic-looking email that appears
to be from your bank, credit card
company, lottery commission, or
representative of a will or estate
fool you into revealing your personal
information or sending money.



CHECK IF THE SITE IS SECURE.

Remember, while more secure sites have a small padlock icon in the lower corner of your browser and the address starts with "https" rather than "http," this does not guarantee that the site is legitimate.

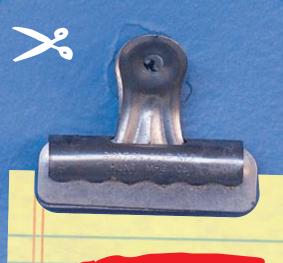
responding to EMAILS that ask you to respond (or your account will be closed) are typically an attempt to steal your personal financial information.

"UNSUBSCRIBING" TO UNSOLICITED
MESSAGES only confirms to spammers
that you're receiving their
emails.

OPENING AN ATTACHMENT FROM
AN UNKNOWN SENDER, especially ".zip"
files, may install viruses that can
damage your computer and possibly
the computers of everyone in your
address book.

INSTALL UPDATED VIRUS AND SPYWARE PROTECTION to prevent your computer from becoming infected.

INSTALL A PERSONAL FIREWALL ON YOUR COMPUTER to prevent hackers from secretly installing spyware or accessing files on your computer.



KEEP ON TOP OF THE LATEST SCAMS

You can access consumer alerts at the Attorney General's website:
www.maine.gov/ag/ and click on
Consumer Protection